Electro Oriente	DIRECTIVA: SEGURIDAD DE LA INFORMACION		
CÓDIGO: D-007	ELABORADO POR: GERENTE DE PLANEAMIENTO, GESTIÓN Y REGULACIÓN	REVISADO POR: GERENTE GENERAL	APROBADO POR: DIRECTORIO
VERSIÓN: 01			
FECHA: 03-07-2015			
N° DE COPIA: 01	PUESTO DE UBICACIÓN: GERENCIA DE PLANEAMIENTO, GESTIÓN Y REGULACIÓN		

1. OBJETIVO

Contar con una Directiva que establezca las Normas de Seguridad de la Información en Electro Oriente S.A. las cuales se deberán cumplir en todo el ámbito de la concesión donde se cuente con equipamiento informático y acceso para manejo de información para evitar el daño, pérdida o mal empleo de la información de la Empresa.

2. ALCANCE

La presente Directiva es de cumplimiento obligatorio para todas las dependencias de Electro Oriente S.A.

3. BASE LEGAL

3.1 Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Código de Buenas prácticas para la gestión de la Seguridad de la Información".

3.2 P17 Tecnología de la Información y Comunicaciones - SGC

4. SITUACIÓN GENERAL

La presente Directiva es de cumplimiento obligatorio para todas las dependencias de Electro Oriente S.A.

- La información es un activo de relevancia para Electro Oriente S.A. y como tal, se debe proteger en todo momento: mientras se procesa, transmite o almacena en múltiples formatos (papel, medios electrónicos, video, etc.).
- La seguridad de Tecnologías de la Información se encarga de proteger la infraestructura computacional y todo lo relacionado a ella: las redes, los sistemas informáticos, los equipos de cómputo y la información que en estos se procesa y almacena, implementando mecanismos que permitan mitigar los ataques externos o internos que puedan dañarlos, alterarlos, sustraerlos o emplearlos en beneficio de intereses contrarios a Electro Oriente S.A.
- Actualmente, debido a los riesgos que expone la integridad, disponibilidad y confidencialidad de la información, la seguridad Tecnologías de la información enfrenta retos, que se incrementan con los avances tecnológicos, situación que ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.
- La Presidencia del Consejo de Ministros, ha normado el uso obligatorio en todas las entidades públicas del código de buenas prácticas para la gestión de la seguridad de la información, descrito en el documento de la Base legal 3.1.
- Es necesario mantener actualizadas las normas de seguridad informática en la Electro Oriente S.A. con ello crear condiciones que permitan minimizar los riesgos de sufrir alteración, mal empleo o pérdida de información.

5. DESARROLLO

Disposiciones Generales

1. El Jefe de TIC y los Supervisores del Departamento de TIC, serán los responsables del cumplimiento de las normas dispuestas en el Anexo "A" de la presente Directiva. Dicho Personal debe ser capacitado en Seguridad de la Información, debiendo seguir obligatoriamente al menos un curso / taller y/o entrenamiento en seguridad de la información la cual debe formar parte del Plan de Capacitación Anual de RRHH.
2. El Jefe de TIC y los Supervisores del Departamento de TIC, deben realizar labores de inspección y control de los sistemas informáticos y de las estaciones de trabajo de manera inopinada, llevándose un registro de las inspecciones realizadas, el cual deberá ser visado por el Gerente de Planeamiento, Gestión y Regulación e Informadas a la Gerencia General.

3. El Jefe de TIC remitirá trimestralmente a la Gerencia de Planeamiento, Gestión y Regulación y a su vez a la Gerencia General el inventario de usuarios con acceso a los sistemas y servicios informáticos: dominio, correo, acceso a las aplicaciones indicándose el perfil y tipos de acceso que se mantiene en la red de datos.
4. Los Usuarios que requieran acceso a los sistemas: dominio, correo, internet, aplicaciones, etc. Solicitarán al Departamento de TIC el acceso correspondiente utilizando los formatos establecidos según los procedimientos del SGC proceso P17 Tecnología de la Información y Comunicaciones, el mismo que será evaluado y autorizado, de ser procedente.
5. El Jefe de TIC remitirá a la Gerencia de Planeamiento, Gestión y Regulación y a la Gerencia General, propuestas para la implementación y la impartición de charlas y/o talleres para la concientización del personal sobre la importancia de la seguridad informática en Electro Oriente S.A. abordando la temática de amenazas, ataques y vulnerabilidades que ponen en riesgo, las consecuencias administrativas y legales del incumplimiento de las normas establecidas de acuerdo a lo descrito en las referencias (a). Asimismo, deberá llevarse un registro firmado del personal asistente, verificando que todo el personal con acceso a los medios informáticos las reciba.
6. El Jefe TIC y los Supervisores TIC tendrán la administración y el control de los recursos de Tecnologías de la Información, debiendo hacer suscribir a todo el personal con acceso a los sistemas el formato de aceptación de los términos de empleo de los Sistemas de Tecnologías de La Información y Comunicaciones Anexo B
7. El personal sin autorización de acceso a medios informáticos, no deberá hacer uso de los mismos, la contraposición a lo dispuesto se considerara falta grave.
8. Las áreas usuarias que requieran la asignación de equipos de cómputo, deben suscribir un acta de asignación según lo estipulado los procedimientos del SGC proceso P17 Tecnología de la Información y Comunicaciones.

Disposiciones Específicas

Gerencia General

En las acciones de control que realice la Empresa, verificará el estricto cumplimiento de las normas de seguridad informática anexo "A" de la presente Directiva, debiendo aplicar los procesos administrativos correspondientes de acuerdo al RIT.

El Gerente de Planeamiento Gestión y Regulación

1. Supervisará el cumplimiento de lo dispuesto en la presente Directiva.
2. Evaluará los requerimientos que sean propuestos por el Departamento de TIC para mejorar las condiciones de seguridad de la información en la Empresa, recomendando a la Gerencia General sobre la atención de los mismos.

Departamento de Recursos Humanos

1. Programará las charlas y/o talleres de capacitación en seguridad informática para los usuarios de Electro Oriente el mismo que deberá dictarse por el Departamento de TIC y/o especialistas externos.
2. Incluirá a todo el personal aspectos de seguridad informática, con la finalidad de que el personal conozca la temática de tecnología de la información, las normas de seguridad que se deben cumplir, la importancia de las mismas y las consecuencias administrativas y legales de su incumplimiento.
3. Capacitará en forma anual al personal del Departamento de TIC en la temática de seguridad informática, con la finalidad de mantenerlo actualizado sobre las estrategias existentes, las cuales sean implementadas en Electro Oriente S.A.

Departamento de TIC

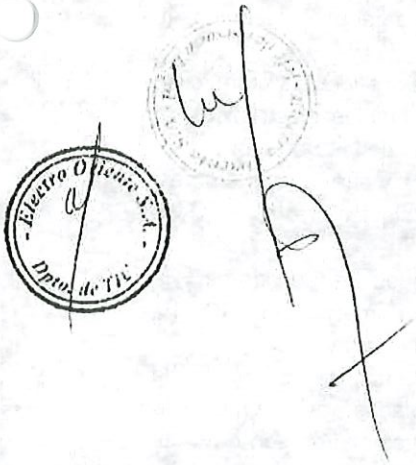
1. Dispondrá del control de archivos y dispositivos de almacenamiento (memorias flash, CD, DVD, impresoras). Para ello, se deberá adquirir la tecnología adecuada y compatible; así como, implementar las políticas de seguridad que regulen el acceso y uso de estos dispositivos. La información considerada relevante se almacenará en un

servidor de archivos implementado y protegido para tal fin, bajo estricta supervisión de los Supervisores TIC.

2. Es el responsable de la operación y mantenimiento de los diferentes sistemas computacionales: recursos de hardware, software y comunicaciones que además implementa los mecanismos de seguridad de la información en el ámbito del dominio elor.com.pe.
3. Propondrá las políticas, normas y procedimientos de seguridad informática en la Electro Oriente SA para su aprobación, ejerciendo estricto control y supervisión del uso de la red y de otras redes informáticas autorizadas en la Empresa.
4. Realizará inspecciones sobre seguridad informática a los Departamentos, Oficinas y en las Unidades en forma programada, inopinada o a requerimiento de las mismas.
5. Brindará el apoyo técnico a las Unidades de Negocio y Servicios eléctricos al ser solicitado por el Encargado de la sede.
6. Brindará charlas sobre Seguridad Informática al Personal y todo usuario de los diferentes sistemas informáticos, las cuales contemplarán las normas de seguridad como las consecuencias administrativas y legales de su incumplimiento, a fin de concientizar al personal de la Empresa.
7. Anulará el acceso a los servicios de correos web externos y/u otros servicios de internet que podrían ser potencialmente riesgosos a la seguridad de la información o de los sistemas informáticos de la Empresa. El único sistema de correo electrónico autorizado a emplearse en la red será el dominio elor.com.pe. Los accesos para las cuentas públicas de personal externo deberán ser debidamente justificadas y aprobadas por la Gerencia General.

6. ANEXO

- "A" Normas de Seguridad Informática en Electro Oriente S.A.
- "B" Formato de Aceptación de los Términos de Empleo de los Sistemas de Información y Comunicaciones de Electro Oriente S.A.



000088

ANEXO "A"

NORMAS DE SEGURIDAD INFORMÁTICA EN ELECTRO ORIENTE S.A.

La Gerencia General de Electro Oriente S.A. deberá disponer y verificar que la comunidad de usuarios de los sistemas informáticos, cumplan con las normas que a continuación se detallan para resguardar la información en las estaciones de trabajo y redes informáticas de la Institución:

1. Está prohibido almacenar información clasificada y confidencial para ELOR en dispositivos de almacenamiento personales.
2. Se deberá restringir y controlar el acceso a información clasificada, de forma que esté disponible sólo para el personal autorizado.
3. Está prohibido instalar aplicaciones a través de software de copias ilegales.
4. Está prohibido descargar y/o instalar software sin licencia (freeware, shareware). La descarga e instalación de estos softwares puede facilitar el ingreso de virus, spyware, troyanos o archivos incompatibles con el sistema.
5. Está prohibido contestar mensajes SPAM (correo electrónico publicitario, no solicitado). Asimismo, no deberán responderse los mensajes que solicitan datos personales, ni reenviar mensajes con falsos contenidos tales como ofertas de premios, dinero, solicitudes de ayuda caritativa o advertencias de virus, etc. Todos ellos provenientes de fuentes desconocidas.
6. Está prohibido el uso de Chat y páginas sociales, el uso de estos medios está reservado a indicación expresa de la Gerencia General.
7. Está prohibido el empleo de software o mecanismos para la manipulación de direcciones de red, de analizadores del tráfico, herramientas de rastreo de puertos, detectores de vulnerabilidades o cualquier otro tipo de programa o hardware que pueda afectar la seguridad de la información de la Institución, la topología o la estructura lógica de la red de datos.
8. El uso de estas herramientas sólo está permitido al personal especializado del Departamento de TIC de la Empresa.
9. Está prohibido y es ilegal modificar las cabeceras de los mensajes de correo electrónico, alterando el origen del mensaje (remitente, fecha, hora, dirección IP, ruta del envió del mensaje, etc.).
10. Está prohibido el envío masivo de mensajes o información (spam), las actividades comerciales privadas, la propagación de correos tipo encadenadas, el uso de los medios electrónicos con fines proselitistas, con contenidos de agresión y que atenten la integridad de las personas.
11. Está prohibido el envío de imágenes o videos que atenten contra la moral y buenas costumbres.
12. Está prohibido tener almacenados videos o fotos de pornografía o cualquier otro material que atente contra la moral y buenas costumbres.
13. Es de carácter obligatorio tener instalado un software antivirus en todos los servidores y las estaciones de trabajo, el cual debe ser autorizado por la Departamento de TIC. Las actualizaciones del antivirus serán configuradas por soporte técnico de las sedes.
14. Es obligatorio usar claves de acceso a la red o dominio, correo y sistemas de información las cuales deben de tener como mínimo de OCHO (08) caracteres, conformadas por la combinación de números, caracteres especiales, letras mayúsculas y minúsculas. Las claves son de índole personal, confidencial e intransferibles por que no deben ser escritas en papel ni estar asociadas a datos comunes del usuario, tales como la fecha de nacimiento, apelativos, nombres de familiares, etc. No debe emplearse la misma clave para diferentes sistemas.
15. Se deberá cambiar toda clave de acceso como máximo, cada NOVENTA (90) días.
16. Se deberá verificar que todo software instalado provenga de fuentes conocidas y seguras.

Electro Oriente S.A. Dpto. de TIC

Electro Oriente	DIRECTIVA: SEGURIDAD DE LA INFORMACION		
CÓDIGO: D-007	ELABORADO POR: GERENTE DE PLANEAMIENTO, GESTIÓN Y REGULACIÓN	REVISADO POR: GERENTE GENERAL	APROBADO POR: DIRECTORIO
VERSIÓN: 01			
FECHA: 03-07-2015			
N° DE COPIA: 01	PUESTO DE UBICACIÓN: GERENCIA DE PLANEAMIENTO, GESTIÓN Y REGULACIÓN		

17. Se deberá limitar la transmisión de datos de uso personal en toda la red de la Empresa, con el fin de evitar la congestión de las mismas. Estando prohibida la conexión de emisoras de radio o de televisión a través de Internet; así como, la descarga o distribución de archivos de audio y video de uso personal.
18. Está prohibido el uso de dispositivos magnéticos o digitales de grabación de información (USB, Reproductores mp3, DVD, CD, etc.). Cuando por razones del servicio se requiera, será con autorización de los Gerentes y/o Jefaturas, llevándose un registro para control de las autorizaciones.
19. Ante cualquier incidencia de seguridad informática, se deberá informar al Departamento de TIC, con la finalidad de determinar el impacto ocasionado y tomar las medidas de seguridad correspondiente.
20. Todos los sistemas y aplicaciones deberán instalarse y configurarse de manera personalizada, para evitar la creación de usuarios y claves por defecto.
21. No deberá activarse la opción de recordar o guardar contraseña de los sistemas y/o aplicaciones, para evitar el ingreso de un usuario no autorizado.
22. No se deberá abrir ningún archivo adjunto a un mensaje de correo electrónico de remitente desconocido o con doble extensión.
23. La clave de acceso o contraseña es PERSONAL e INTRANSFERIBLE, por lo que el usuario deberá modificarla de manera inmediata ante la suposición o certeza de que un tercero ha llegado a conocerla. Toda acción realizada es responsabilidad del usuario de la cuenta. El titular de la cuenta de usuario que preste su clave a otra persona, será sancionado al igual que la personal que utilizó dicha clave; por atentar contra la seguridad de información de la Empresa.
24. El acceso a la red, sistemas y servicios debe realizarse únicamente con las credenciales que el departamento TIC haya asignado. Se considera falta grave el compartir y/o utilizar cuentas de usuarios que no hayan sido asignadas de manera directa.
25. El Departamento de TIC bloqueara automáticamente las cuentas de los usuarios del Personal cuando estos se encuentren en condición de cese de funciones, de licencia, vacaciones o que por alguna razón no se encuentran en situación de labores efectiva. Para ello la Gerencia de Administración y Finanzas a través del Departamento de Recursos Humanos deberá alcanzar oportunamente la relación de los trabajadores en tales situaciones.
26. Para el acceso a los servicios de la red, se admitirán como máximo cuatro (04) intentos fallidos de empleo de la clave de acceso, bloqueándose posteriormente por un lapso de dos (02) horas.
27. Únicamente están permitidos a utilizar los servicios informáticos de la Empresa aquellos usuarios, o grupos de usuarios, que estén expresamente autorizados.
28. Todos los equipos que se conectan a la red deben recibir una dirección IP dinámica y un nombre de red asignados por el servidor controlador del dominio. Las direcciones IP reservadas sólo están autorizadas para los equipos, servidores u otros equipos de comunicación que requieran obligatoriamente este tipo de dirección.
29. Los equipos que accedan a la red en forma remota (usuarios autorizados), sólo podrán hacerlo a través de los medios proporcionados por el Departamento de TIC y cumpliendo con las normas de seguridad obligatorias para los usuarios locales del dominio elor.com.pe.
30. Todos los equipos de administración y seguridad de la red serán instalados, configurados y administrados por el Departamento de TIC de Electro Oriente S.A.
31. Ante la necesidad de implementar una red de área local (LAN), el Departamento de TIC debe indicar los aspectos más relevantes del diseño técnico (infraestructura, equipamiento, aplicaciones a instalar, sistema de control de acceso, uso de cada estación de trabajo, etc.) quienes emitirán un informe técnico con las correspondientes recomendaciones.

Electro Oriente S.A. Dpto. de TIC

32. Toda habilitación de nuevos puntos de red se hará en coordinación con personal técnico del Departamento de TIC.
33. En caso de que algún equipo de tercero tenga acceso a la red y que utilice algún software que entre en conflicto con la ejecución de las aplicaciones de gestión de la red, dicho software deberá ser desinstalado.
34. Para la conexión de equipos de cómputo de terceros se debe requerir la autorización del Departamento de TIC, el personal técnico evaluara la factibilidad de su inclusión en la red para lo cual los equipos deben de contar con software licenciado y un antivirus actualizado de no contar con estas condiciones bajo ninguna consideración se procederá el requerimiento.
35. Todas las estaciones de trabajo que formen y/o que tengan acceso a de la red de Electro Oriente (personal propio, terceros y contratistas) serán sujetas a la aplicación de las políticas de seguridad impuestas por Departamento de TIC, de vulnerarse estas restricciones se considerar falta grave imputándose las acciones que correspondan.
36. Por defecto los usuarios con acceso a la red tiene restringido la libre navegación a Internet, el acceso a tal servicio debe ser requerido al departamento TIC con el formato declarado en el SGC P17 Tecnología de la Información y Comunicaciones, los perfiles a aplicar estarán en concordancia a las labores que se demanden.
37. Toda persona que incumpla las normas descritas anteriormente, será sancionada de acuerdo al grado de responsabilidad y magnitud de la falta cometida por atentar contra la seguridad de información, sin perjuicio de las acciones administrativas y/o legales de la empresa pueda realizar en contra de los infractores.

Electro Oriente S.A. Dpto. de TIC

Electro Oriente Generando Progreso	DIRECTIVA: SEGURIDAD DE LA INFORMACION		
CÓDIGO D-007	ELABORADO POR: GERENTE DE PLANEAMIENTO, GESTIÓN Y REGULACIÓN	REVISADO POR: GERENTE GENERAL	APROBADO POR: DIRECTORIO
VERSIÓN 01			
FECHA 03-07-2015			
N° DE COPIA: 01	PUESTO DE UBICACIÓN: GERENCIA DE PLANEAMIENTO, GESTIÓN Y REGULACIÓN		

ANEXO "B"

FORMATO DE ACEPTACIÓN DE LOS TÉRMINOS DE EMPLEO DE LOS SISTEMAS DE COMUNICACIONES E INFORMÁTICA DE LA EMPRESA ELECTRO ORIENTE SA.

Yo (1)....., identificado con DNI: (2) ..... DECLARO QUE CONOZCO Y ACEPTO sin reserva alguna los términos de la Directiva de Seguridad de la Información, comprometiéndome al cumplimiento estricto de lo normado.

Asimismo, declaro que tengo conocimiento y acepto que Electro Oriente S.A en resguardo de sus intereses, emplee programas para el control del tráfico en la red y la protección de la información para identificar el intento de uso malicioso o no autorizado; así como, tentativas de modificar o causar daños a otros usuarios, a los servicios de comunicación, servidores, información u otros equipos informáticos dentro de la Empresa.

Conozco y acepto también, que los sistemas de comunicación e información de Electro Oriente S.A., están sujetos a MONITOREO, CONTROL Y AUDITORÍA, pudiendo emplearse esta información cuando corresponda para fines de DENUNCIA en la vía civil y penal, y para la aplicación de sanciones administrativas a los infractores.

.....
(FECHA)

.....
Antefirma
FIRMA

LEYENDA:

(1) Apellidos y Nombres del Personal que realiza trabajos en sistemas de comunicaciones e información.
(2) N° del Documento Nacional de Identidad (DNI).